UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/683,582	10/09/2003	Yung Chang Liang	TRNDP010	9453

22434 7590 07/06/2007

BEYER WEAVER LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER	
NGUYEN, KHOI	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
07/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/683,582	**Applicant(s)** LIANG ET AL.	
	Examiner Khoi Nguyen	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *1* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06/07/2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *04/02/2007*.
4) ☒ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosures

1. The IDS filed on 5/07/2007 has been considered by the examiner.

2. Claims 1-30 are pending in the application.

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Specification

3. Objections to specification have been withdrawn due to applicant amendment filed on 6/14/2007.

Claims Objections

4. Objections on claim 3, 17, and 20 have been withdrawn due to applicant amendment filed on 6/14/2007.

Double Patenting

5. The nonstatutory double patenting rejection has been withdrawn in view of amendments made in the co-pending application no. 10/683579 filed on 2/20/2007.

Claim Rejections – 35 USC § 112

6. Claim rejections under USC 112 have been withdrawn in view of the amendment filed on 6/14/2007.

Response to Amendment

7. Applicant's amendment filed on 6/27/2007 has been fully considered and is entered.

Response to Arguments

8. Applicant's arguments, see page 11, filed 06/07/2007, with respect to the rejection(s) of claim(s) 1 and 11 under 35 USC 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Suuronen, Doughlas, and further in view of White.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-30 are rejected under 35 USC 103(a) as unpatentable over Suuronen et al. (US PGPub No. 2003/0145228), hereafter "Suuronen", and in view of Douglas et al. (US Pat. No. 6269400), hereafter "Douglas", further in view of White et al. ("Anatomy of a Commercial-Grade Immune System, IBM Research White Paper, 1999, http://www.research.ibm.com/antivirus/SciPapers/White/Anatomy/Anatomy.PDF), hereafter "White", and further in view of Cass ("Anatomy of Malice", Spectrum IEEE, Nov. 2001, vol. 35, issue 11, pages: 56-60), hereafter "Cass".

11. With regard to claim 1, Suuronen discloses a network virus defense system (abstract), comprising:

A network virus/worm sensor (Fig. 1 – item 14, 22, and 24, [0020] lines 1-16) operable in a number of modes arranged to detect a computer virus or a computer worm in the network ([0020] lines 1-16, first and second type of packet determines whether the instant packet would be passed directly to the destination or be forwarded to virus scan engine for further analysis; thus, it indicates that the firewall is operating in a number of modes) such that the bandwidth of the network is substantially unaffected in a first mode ([0007] lines 5-10, [0020] lines 2-9 being able to process packets in real time would mean that the bandwidth is unaffected by this process), and wherein when the virus sensor detects the computer virus, the virus sensor switches to a second mode ([0019], lines 27- 39, sending second type of packets to virus scanning engine indicates second mode), wherein the data packet are not copied and wherein a subset of data packet determined to be infected or suspected of being infected are not returned to the network ([0021] lines 28-34, dropped data packets being received by Firewall indicates that infected packets are not returned to the network).

A controller (Fig. 1: items 14 and 16) storing a rules engine used to store and source a plurality of detection rules for detecting computer viruses and worms (Fig. 1 items 22 and 24, virus scanning engine couple with virus detection database form rules engine to detect computer viruses and worms, [0021] lines 5-6).

A server for virus cleaning agents from known viruses subsequently analyzed (Fig. 1: item 22 and 24).

Suuronen does not disclose a network virus sensor self registration module coupled to the network virus/worm sensor arranged to automatically self register the associated network virus/worm sensor.

Douglas, on the other hand, discloses a network virus sensor self registration module coupled to the network virus/worm sensor (col. 3, lines 28-31, HTTP server reads on self registration module) arranged to automatically self register the associated network virus/worm sensor (col. 4, lines 65-68).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify Suuronen by the methods of self registration coupled to the network virus/worm sensor automatically self register the associated network virus/worm sensor as taught by Douglas, and would be motivated to conduct automatically discovery and registration of available agents on a distributed network (Douglas, col. 2, lines 38-39).

Neither Suuronen nor Douglas discloses the data packets are not removed from or added to network traffic, but are copied; a controller to detect viruses and worm using statistical result; a server for virus cleaning agent from unknown viruses, and an anti-virus agent creation module.

White discloses the data packets are not removed from or added to network traffic but are copied (Section "Epidemics and Floods", page 2, second paragraph, lines 1-3; Section "Cure Distribution", page 13, second paragraph, lines 2-5); a controller to detect viruses and worm using statistical result (Section "Analysis", page 21, lines 5-6, footnote 10); a server for virus cleaning agent from unknown viruses (Fig. 2, page 11, Analysis center), and an anti-virus agent creation module (section "Cure Distribution", page 13, first paragraph, lines 1-4).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the teachings of Suuronen and Douglas to include the method of data packets are not removed from or added to network traffic, but are copied; a controller to detect viruses and worm using statistical result; a server for virus cleaning agent from unknown viruses and an anti-virus agent creation module, as taught by White and would be motivated to provide an immune system that can find , analyzed, and cure previously unknown viruses faster than the viruses themselves can spread (White, page 2, first paragraph, lines 1-2).

Furthermore, neither Suuronen, Douglas, nor White discloses the creation of a detection module, an infection module and a payload.

Cass discloses create a detection module, an infection module and a payload (Section "Source of Mischief" page 59).

It would have been obvious for one of the skill in the art to modify the teachings of Suuronen, Douglas, and White to include the creation of a detection module, an infection module and a payload as taught by Cass, and would be motivated to provide an effective defense by understanding the cause and mechanism of infection (Cass, page 56, paragraph 5, lines 1-3).

12. With regard to claim 11, limitations of the instant claim have been discussed in claim 1 above with the exception of the following limitation.

Neither Suureno, Douglas, nor White discloses creating a detection module that detects whether a client device is infected with a virus and triggers the introduction of an anti-virus infection module so that the virus in the client device is overwritten and an anti-virus payload created based on features of the selected computer virus and perform as cleaning/repairing payload capable of cleaning and repairing damage done to the client device.

Cass, on the hand, discloses a detection module for detecting whether a client device is presently infected with a virus, triggers the introduction of an anti-virus infection module so that the virus in a client device is overwritten, wherein an anti-virus agent payload, created based on features of the selected computer virus, performs as a cleaning/repairing payload capable of cleaning and repairing damage done to the client device, the payload also capable of inoculating the client device against the virus in cases where the client device was not infected by the computer virus ("Source of Mischief" section, page 59).

It would have been obvious for one of the skill in the art to modify the teachings of Suureno, Douglas, and White to include creating a detection module that detects whether a client device is infected with a virus and triggers the introduction of an anti-virus infection module so that the virus in the client device is overwritten and an anti-virus payload created based on features of the selected computer virus and perform as cleaning/repairing payload capable of cleaning and repairing damage done to the client device as taught by Cass, and would be motivated to provide an effective defense by understanding the cause and mechanism of infection (Cass, page 56, paragraph 5, lines 1-3).

4. With regard to claim 21, Suuronen discloses a network having a number of servers and associated client devices, a computer program product ([0007] line 4) of a network virus defense system (Abstract) that includes a network virus/worm sensor (Fig. 1 – item 14, 22, and 24, [0020] lines 1-16) operable in a number of modes arranged to detect a computer virus or a computer worm in the network ([0020] lines 1-16, first and second type of packet determines whether the instant packet would be passed directly to the destination or be forwarded to virus scan engine for further analysis; thus, it indicates that the firewall is operating in a number of modes).

Computer readable medium for storing the computer code ([0007], line 4).

However, neither Suuronen, White nor Cass discloses computer code of automatically self registering the associated network virus/worm sensor by a network virus sensor self registration module coupled to the network virus/worm sensor.

Douglas, on the other hand, discloses computer code for automatically self registering the associated network virus/worm sensor by a network virus sensor self registration module (col. 4, lines 65-68) coupled to the network virus/worm sensor (col. 3, lines 28-31, HTTP server reads on self registration module).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify Suuronen by the methods of self registration coupled to the network virus/worm sensor automatically self register the associated network virus/worm sensor as taught by Douglas, and would be motivated to conduct automatically discovery and registration of available agents on a distributed network (Douglas, col. 2, lines 38-39)

13. With regard to claims 2, 12, and 22, Suuronen discloses an initialization phase of the network virus/worm sensor ([0021] lines 14-15 dynamically updated with virus updates indicates the initialization phase).

However, neither Suuronent, White nor Cass discloses the network virus/worm self registration module collects selected network environmental information and network configuration information.

Douglas, on the other hand, discloses disclose the network virus/worm self registration module collects selected network environmental information and network configuration information (col. 4, lines 61-64, host name and operating system indicate network environmental and configuration information).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the teachings of Suuronen, White, and Cass to include self registration coupled to the network virus/worm sensor automatically self register the associated network virus/worm sensor as taught by Douglas and would be motivated to conduct automatically discovery and registration of available agents on a distributed network (Douglas, col. 2, lines 38-39).

14. With regard to claims 3, 13, and 23, Suuronen discloses a system wherein when the distributed network is an IP based type network ([0019], lines 4-5, TCP/IP protocol indicates the network is an IP based netwrok). However, neither Suuronen, White nor Cass discloses the selected network environmental information includes an IP address for all of the relevant client devices included in the IP-based network.

Douglas, on the other hand, discloses the selected network environmental information includes an IP address for all of the relevant client devices included in the IP-based network (col. 3, lines 61-64).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the teachings of Suuronen, White, and Cass by including an IP address for all the relevant client devices included in the network, as taught by Douglas, and would be motivated to conduct automatically discovery and registration of available agents on a distributed network (Douglas, col. 2, lines 38-39).

15. With regard to claims 4, 14, and 24, Suuronen discloses the network virus/worm sensor (Fig. 1 – items 14, 22 and 24, [0020] lines 1-16). However, Suuronen does not disclose the network configuration information includes self configuration information related to an appropriate IP address for the network virus/worm sensor.

Douglas, on the other hand, discloses the network configuration information includes self configuration information related to an appropriate IP address for the network virus/worm sensor (col. 4, lines 61-64, host name indicates self configuration).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the teachings of Suuronen, White, and Cass to include the network configuration information includes self configuration information related to an appropriate IP address for the network virus/worm sensor, as taught by Douglas, and would be motivated to conduct automatically discovery and registration of available agents on a distributed network (Douglas, col. 2, lines 38-39).

16. With regard to claims 5, 15, and 25, Suuronen does not disclose the network configuration information includes locations of all relevant server computers.

Douglas, on the other hand, discloses the network configuration information includes locations of all relevant server computers (col. 3, lines 60-62, list of IP addresses indicates locations of all relevant server computers).
It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the teachings of Suuronen, White, and Cass to include the network configuration information includes locations of all relevant server computers, as taught by Douglas, and would be motivated to conduct automatically discovery and registration of available agents on a distributed network (Douglas, col. 2, lines 38-39).

17. With regard to claims 6, 16, and 26, Suuronen discloses selected ones of the relevant server computers (Fig. 1, [0009] lines 1-5, a firewall and virus scanning engine indicates the selected relevant server computers) are identified as controllers (Fig. 1 items 14 and 16, [0020] the combination of the firewall and Packet Classification Database act as a traffic controller to determine which packets get transferred to the network and which packets get forwarded to the Virus Scanning Engine).

18. With regard to claims 7, 17, and 27, Suuronen discloses each of the identified controllers (Fig. 1 items 14 and 16) includes a rules engine used to store and source a plurality of detection rules for detecting computer viruses and worms (Fig. 1 items 22 and 24, virus scanning engine couple with virus detection database form rules engine to detect computer viruses and worms, [0021] lines 5-6).

However, neither Suuronen, Douglas, nor Cass discloses an outbreak prevention policy (OPP) distribution and execution engine that provides a set of anti-virus policies, protocols, and procedures suitable for use by a system administrator for both preventing viral outbreaks and repairing any subsequent damage caused by a viral outbreak.

White, on the other hand, discloses an outbreak prevention policy (OPP) distribution and execution engine (Fig. 3, page 14, Supervisor, Gateways, and admin system indicates OPP distribution and execution engine) that provides a set of anti-virus policies (page 13, Cure Distribution section, second paragraph, lines 5-8, install the updated virus definition indicates antivirus policies), protocols (page 20, Classification section, first paragraph), and procedures (page 14, second paragraph, lines 4-12) suitable for use by a system administrator for both preventing viral outbreaks and repairing any subsequent damage caused by a viral outbreak (page 13, Cure distribution section, first paragraph and second paragraph lines 5-7).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the teachings of Suuronen, Douglas, and Cass to include an outbreak prevention policy (OPP) distribution and execution engine that provides a set of anti-virus policies, protocols, and procedures suitable for use by a system administrator for both preventing viral outbreaks and repairing any subsequent damage caused by a viral outbreak, as taught by White and would be motivated to provide an immune system that can find , analyzed, and cure previously unknown viruses faster than the viruses themselves can spread (White, page 2, first paragraph, lines 1-2).

19. With regard to claims 8, 18, 28, Suuronen discloses during the initialization phase ([0021] lines 14-15 dynamically updated with virus updates indicates the initialization phase), each of the rules engines (Fig. 1 items 22 and 24, virus scanning engine couple with virus detection database form rules engine to detect computer viruses and worms, [0021] lines 5-6) associated with each of the identified controllers (Fig. 1 items 14 and 16) are updated with a set of detection rules for detecting computer viruses and worms ([0021] lines 14-21).

20. With regard to claims 9, 19, and 29, Suuronen discloses during the initialization phase ([0021] lines 14-15 dynamically updated with virus updates indicates the initialization phase) of each of the identified controllers (Fig. 1 items 14 and 16).

However, neither Suuronen nor Douglas discloses each of the outbreak prevention policy distribution and execution engines are updated with a set of anti-virus policies, a set of anti-virus protocols, and a set of anti-virus procedures.

White, on the other hand, discloses each of the outbreak prevention policy distribution and execution engines (Fig. 3, page 14, Supervisor, Gateways, and admin system indicates OPP distribution and execution engine) are updated with set of anti-virus policies (page 13, Cure Distribution section, second paragraph, lines 5-8, install the updated virus definition indicates antivirus policies), protocols (page 20, Classification section, first paragraph), and procedures (page 14, second paragraph, lines 4-12).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the teachings of Suuronen, Douglas, and Cass to include each of the outbreak prevention policy distribution and execution engines are updated with a set of anti-virus policies, a set of anti-virus protocols, and a set of anti-virus procedures, as taught by White and would be motivated to provide an immune system that can find, analyzed, and cure previously unknown viruses faster than the viruses themselves can spread (White, page 2, first paragraph, lines 1-2)..

21. With regard to claims 10, 20, and 30, Suuronen discloses in a first mode the bandwidth of the network is substantially unaffected by the network virus/monitor sensor ([0007] lines 5-10, [0020] lines 2-9 being able to process packets in real time would mean that the bandwidth is unaffected by this process) wherein when the network virus/worm sensor (Fig 1 items 22 and 24) detects a computer virus or a computer worm, the virus/worm sensor switches to a second mode ([0019], lines 27- 39, sending second type of packets to virus scanning engine indicates second mode) such that only those data packets infected by the computer virus are not returned to the network ([0021] lines 28-34, dropped data packets being received by Firewall indicates that infected packets are not returned to the network).

Neither Suuroneno, Douglas, nor Cass discloses the network virus/monitor sensor not removing or adding network traffic but copying data packets.

White discloses the network virus/monitor sensor not removing or adding network traffic but copying data packets (Section "Epidemics and Floods", page 2, second paragraph, lines 1-3; Section "Cure Distribution", page 13, second paragraph, lines 2-5).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the teachings of Suuronen, Douglas, and Cass to include the network virus/monitor sensor not removing or adding network traffic but copying data packets, as taught by White and would be motivated to provide an immune system that can find, analyzed, and cure previously unknown viruses faster than the viruses themselves can spread (White, page 2, first paragraph, lines 1-2).

Conclusion

22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. US PGPub No. 2006/0212572 to Afek et al. (Discloses screening first packet for any malicious signature. If found blocked the source address)

b. US Pat. No. 6711686 to Barrett (Discloses security management tool to gather system information).

c. US Pat. No. 5920698 to Ben-Michael et al. (Discloses automatic detection by a port of the type of device connect to a network).

d. US PGPub No. 2004/0139179 to Beyda (Discloses monitoring and automatically detect faulty network traffic routing conditions).

e. US PGPub No. 2004/0139196 to Butler et al. (Discloses releasing a reservation held by a host on a target device).

23. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Khoi Nguyen whose telephone number is 570-270-1251. The examiner can normally be reached on Mon-Fri (8:30 am – 5:00 pm est) If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

25. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Khoi Nguyen
Art Unit 2132
Date: 6/27/07

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100